InceLink
Security Overview

Secure Connection

HTTPS/SSL — Every page on InceLink is connected using HTTPS and secured using 256-bit encrypted SSL (Secure Sockets Layer). Norton Secured, Powered by VeriSign.

Encryption — Inbound and outbound data is encrypted to ensure the safest transfer to our servers. We use bank-level security to keep your information safe.

Secure Storage and Hosting

InceLink is SSAE16 Type I (formerly SAS70) certified and all data is hosted and managed by Amazon Web Services (AWS) via their secure data centers. Engine Yard provides security layers and continued operations support for our application.

AWS's data center operations have been accredited under:

- ISO 27001
- SOC1/SSAE 16/ISAE 3402 (Previously SAS70 Type II)
- PCI Level 1
- FISMA Moderate
- Sarbanes-Oxley (SOX)

Amazon OpsWorks provides enhanced reliability and security with:

- Daily Backups
- Malware Mitigation
- Safe Harbor Certification
- 99.9% Uptime

Controlled Access

Permission Control — Administrators decide who has access to each folder and set whether they can view or download.

File Access — Files are private by default and can be shared at any time.

No Indexing — We block all search engine and web crawlers from private data.

Comprehensive Activity Tracking

Monitoring — Know when someone views your workspace, views/downloads a file, and more.

Audit Trail — We archive a complete history of every event that has occurred in each Workspace.

Security Features

Watermarking — Enable a watermark on viewed/downloaded documents that includes time, date, user email, and IP address.

DRM — InceLink's proprietary Digital Rights Managment allows users to revoke access to downloaded documents.